

PCT

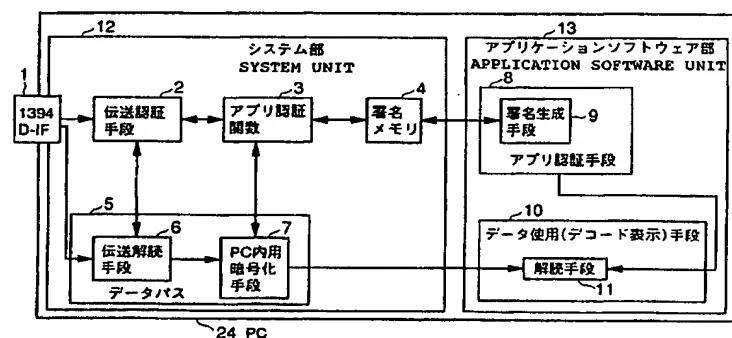
世界知的所有権機関
国際事務局
特許協力条約に基づいて公開された国際出願



(51) 国際特許分類7 G06F 9/06	A1	(11) 国際公開番号 WO00/50989
		(43) 国際公開日 2000年8月31日(31.08.00)
(21) 国際出願番号 PCT/JP00/00956		
(22) 国際出願日 2000年2月21日(21.02.00)		
(30) 優先権データ 特願平11/43870 1999年2月22日(22.02.99) JP		
(71) 出願人 (米国を除くすべての指定国について) 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP] 〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP)		久野良樹(KUNO, Yoshiki)[JP/JP] 〒570-0054 大阪府守口市大枝西町14-26-204 Osaka, (JP)
(72) 発明者; および (75) 発明者/出願人 (米国についてのみ) 武知秀明(WAKECHI, Hideaki)[JP/JP] 〒533-0004 大阪府豊中市上新田3丁目6-17-407 Osaka, (JP)		後藤昌一(GOTOH, Shoichi)[JP/JP] 〒567-0042 大阪府茨木市宇野辺2丁目6-45-710 Osaka, (JP)
山田正純(YAMADA, Masazumi)[JP/JP] 〒570-0011 大阪府守口市金田町6-24-10 Osaka, (JP)		(74) 代理人 弁理士 松田正道(MATSUDA, Masamichi) 〒532-0003 大阪府大阪市淀川区宮原5丁目1番3号 新大阪生島ビル Osaka, (JP)
飯塚裕之(IITSUKA, Hiroyuki)[JP/JP] 〒576-0033 大阪府交野市私市6-25-6 Osaka, (JP)		
西村拓也(NISHIMURA, Takuya)[JP/JP] 〒545-0053 大阪府大阪市阿倍野区松崎町3-9-18-F Osaka, (JP)		(81) 指定国 CN, KR, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)
		添付公開書類 国際調査報告書

(54) Title: COMPUTER AND PROGRAM RECORDED MEDIUM

(54) 発明の名称 コンピュータ及びプログラム記録媒体



2...TRANSMISSION AUTHENTICATION MEANS	7...CIPHERING MEANS FOR INSIDE OF PC
3...APPLICATION AUTHENTICATION FUNCTION	8...APPLICATION AUTHENTICATION MEANS
4...SIGNATURE MEMORY	9...SIGNATURE CREATING MEANS
5...DATA PATH	10...DATA USING (DECODE DISPLAY) MEANS
6...TRANSMISSION DECODING MEANS	11...DECODING MEANS

(57) Abstract

There has been a problem that once copyrighted AV data is delivered to an application software, it is possible for the application software to freely record the AV data, and consequently the copyright cannot be secured. A computer having a system unit (12) and an application software unit (13) and adapted to capture and process copyrighted ciphered data through a digital interface (1), characterized in that the system unit (12) judges if the application software unit (13) is an application software that is right in copyright security, and the system unit (12) delivers the key of the ciphered data to the application software unit (13).

著作権主張されたAVデータが一旦アプリケーションソフトウェアに渡されてしまえば、アプリケーションソフトウェアが自由にAVデータを記録などの処理をすることが可能であり、著作権を守ることが出来ないという課題がある。

システム部12とアプリケーションソフトウェア部13とを備え、デジタルインターフェース1から著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、システム部12は、アプリケーションソフトウェア部13が著作権を守る上において正当なアプリケーションソフトウェアであると判定し、正当なものである場合は、暗号化データの鍵をアプリケーションソフトウェア部13に渡すことを特徴とするコンピュータ。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スードゥ丹
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴー
BG	ブルガリア	GM	ガンビア	MD	モルドavia	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサオ	共和国		TT	トリニダッド・トバゴ
CA	カナダ	HR	クロアチア	ML	マリ	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	UA	ウクライナ
CG	コンゴー	ID	インドネシア	MR	モーリタニア	UG	ウガンダ
CH	スイス	IE	アイルランド	MW	マラウイ	US	米国
CI	コートジボアール	IL	イスラエル	MX	メキシコ	UZ	ウズベキスタン
CM	カメルーン	IN	インド	MZ	モザンビーク	VN	ベトナム
CN	中国	IS	アイスランド	NE	ニジエール	YU	ユーゴースラヴィア
CR	コスタ・リカ	IT	イタリア	NL	オランダ	ZA	南アフリカ共和国
CU	キューバ	JP	日本	NO	ノルウェー	ZW	ジンバブエ
CY	キプロス	KE	ケニア	NZ	ニュージーランド		
CZ	チェコ	KG	キルギスタン	PL	ポーランド		
DE	ドイツ	KP	北朝鮮	PT	ポルトガル		
DK	デンマーク	KR	韓国	RO	ルーマニア		

明細書

コンピュータ及びプログラム記録媒体

技術分野

本発明は、データを記録再生するコンピュータ及びプログラム記録媒体に関するものである。

背景技術

音声情報や映像情報をデジタル化して伝送するネットワークが開発されてきている。音声情報や映像情報を伝送し、視聴するためにはリアルタイムにデータを伝送する必要がある。

このようなリアルタイムデータ伝送を行うネットワークの標準として I E E E 1 3 9 4 が提案され、現在広く用いられるようになった。I E E E 1 3 9 4 は、家庭用デジタルV C Rを始め、多くのデジタル映像音声機器に外部用インターフェースとして搭載されている。V C Rにおいては、I E E E 1 3 9 4 を用いることにより、外部機器からV C Rの動作制御を行ったり、また外部機器からV C Rにデータを送信し、V C Rにおいて記録することや再生することなども可能となった。

一方P Cにおいては、マルチメディア技術の進展、大容量のハードディスクや光磁気ディスクなどの記録媒体の出現により、映像情報や音声情報をも処理できるようになった。すなわちP Cは映像情報や音声情報の記録再生装置やモニタとしても機能できるようになった。P Cの標準O SであるW i n d o w s 9 8などにおいてはI E E E 1 3 9 4 がサポ

ートされており、VCRなどのディジタル映像音声機器とPCで互いにAVデータのやりとりが可能となっている。このように今後ディジタル映像音声機器とPCとの融合がますます進展していくものと思われる。

PCで映像情報や音声情報を扱うためには、映像情報や音声情報を処理するアプリケーションソフトウェアをPCにインストールしておく必要がある。映像音声機器から送られてくるAVデータはPCの内部に入力され、PCにインストールされているアプリケーションソフトウェアによって表示、記録、再生などの処理が行われる。例えばアプリケーションソフトウェアが記録を行う機能を持つものであれば、映像音声機器から送られてきたAVデータはPCに入力され、アプリケーションソフトウェアによって、ハードディスクや光磁気ディスクなどの記録媒体に記録される。このようにAVデータを処理できるアプリケーションソフトウェアは様々であり、アプリケーションソフトウェアをインストールすることによってPCにAVデータを処理するための記録、再生、表示、加工など多種多様な機能を付加することができる。

一方AVデータには複製を禁止する、一世代のみ複製を許可するなどの著作権主張されたAVデータがある。このように著作権主張されたAVデータはVCRなどのディジタル映像音声機器ではその著作権の意図するところを守って記録、再生などが行われる。例えば複製を禁止するというAVデータに対してはVCRは記録をしない。ところが一世代のみ複製を許可するというAVデータであればVCRは記録することができる。このようにAVデータを複製できるか否かは、VCRとSTB(衛星放送受信器)などのAVデータの送り手となる機器との間で認証

や著作権に基づく利用許諾情報によって確認する。

しかし、現在のPCでは、著作権主張されたAVデータに対して、PCがその著作権を守ろうとしてもPCにインストールされているアプリケーションソフトウェアの機能によって、PCに記録、再生、表示などの多種多様の機能を持たせることが出来るため、著作権主張されたAVデータが一旦アプリケーションソフトウェアに渡されてしまえば、アプリケーションソフトウェアが自由にAVデータを記録などの任意の処理をすることが可能であり、著作権を守ることが出来ないという問題がある。

また、アプリケーションソフトウェアに対して、著作権主張されたAVデータを処理するためのライセンスを付与する仕組みを作ったとしても、アプリケーションソフトウェアが不正に改竄されて、著作権が守られない場合がある。アプリケーションソフトウェアの不正改造を防ぐため、タンパレジスタンントの方式をアプリケーションソフトウェアに実装すれば、効果的に著作権は守られる。しかしこの場合も一旦タンパレジスタンントの方式が不正なユーザによって破られれば、PCの構造やOS、アプリケーションソフトウェアの構成などを大きく変える必要が生じ、損失が大きいという問題がある。

また、上述したようなライセンスを与えられていないアプリケーションソフトウェアが著作権主張されたデータを不正に扱った場合、不正なアプリケーションソフトウェアにより複製され流出したデータから出所のアプリケーションソフトウェアを特定することができない。すなわち不正なアプリケーションソフトウェアが知られた後、不正なアプリケ

ションソフトウェアを再び使おうとすると、それを検知し排斥することができない。つまり著作権保護に対して不正なソフトウェアを確認し、排斥することが不可能であるという問題がある。

また、ソフトウェアによる不正利用の特徴はソフトウェアのコピー等により、不正利用の方法が低コストで広く流布し得ることである。そのため、たとえ不正流出の出所を特定できたとしても、ハードウェアの場合に用いられる不正な機器をその特定機器毎に排除する方式は有効でないという課題がある。例えばタンパレジスタントのチェックを回避出来る、改竄されたアプリケーションのコピーが流通したり、またはあるタンパレジスタントのチェック方式を回避する方法が、発見され流通した場合には、個別のコンピュータ毎に排除する従来の方式では不正を防止出来ない上、正常なアプリケーションさえ利用出来なくなる可能性がある。

さらに、以上のような観点から、不正流出の仕組みを備えたコンピュータによる不正流出が一旦発覚した場合には、コンピュータやOS自体に対してAVデータの使用を禁止したり、コンピュータやOS自体の改変が必要になるなど広範囲に不利益が生じ、非常に大きなコストを要することは明らかである。

このように、著作権主張されたデータが不正配布された場合に以後容易に不正利用を防止する方法がないという問題がある。

本発明は、著作権主張されたデータに対してアプリケーションソフトウェアが著作権に反する処理を行うことが出来、著作権が守られないという課題と、アプリケーションソフトウェアが不正改造などにより、著作権主張に反することが行われるという課題と、不正なアプリケーションソフトウェアが発生した場合に、著作権保護に対して不正なアプリケーションソフトウェアを確認し、排斥することが不可能であるという課題と、タンパレジスタンントのチェック方式を回避出来る改竄されたアプリケーションのコピーが流通した場合、従来の方式では不正を防止出来ないという課題と、不正流出の仕組みを備えたコンピュータによる不正流出が発覚した場合には、これを排除するために非常に大きなコストを要するという課題を考慮し、著作権主張されたデータに対しては著作権を守り、アプリケーションソフトウェアの不正な改竄に対処し、不正なアプリケーションソフトウェアに対して、そのアプリケーションソフトウェアを確認し、排斥し、不正な流出をコストをかけずに排除することができるコンピュータ及びプログラム記録媒体を提供することを目的とするものである。

上述した課題を解決するために、第1の本発明（請求項1に対応）は、システム部とアプリケーションソフトウェア部とを備え、

ディジタルインターフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、

前記システム部は、前記アプリケーションソフトウェア部が著作権を守る上において正当なアプリケーションソフトウェアであると判定し、正当なものである場合は、暗号化データの鍵をアプリケーションソフ

トウェア部に渡すことを特徴とするコンピュータである。

また第2の本発明（請求項2に対応）は、前記システム部における判定は、前記システム部とアプリケーションソフトウェア部との間における認証で行われることを特徴とする第1の発明に記載のコンピュータである。

また第3の本発明（請求項3に対応）は、前記システム部における判定は、不正なまたは正当なアプリケーションソフトウェアが載っているCRL（C e r t i f i c a t i o n R e v o c a t i o n L i s t）で行うことを特徴とする第1の発明に記載のコンピュータである。

また第4の本発明（請求項4に対応）は、前記システム部は前記暗号化された鍵を外部との認証結果により得て、前記暗号化されたデータを復号し、再度その鍵または別の鍵で復号化されたデータを再暗号化することを特徴とする第1～3の発明のいずれかに記載のコンピュータである。

また第5の本発明（請求項5に対応）は、前記システム部はタンパ確認関数を有しており、前記アプリケーションソフトウェア部のアプリケーションソフトウェアにタンパコードが埋め込まれており、前記システム部は前記アプリケーションソフトウェア部からタンパコードを読みとり、タンパ確認関数を用いて、アプリケーションソフトウェアの改竄の有無を判定し、それをを利用して、改竄されていることが判明した場合は、その結果を知らせることを特徴とする第1～4の発明のいずれかに記載のコンピュータである。

また第6の本発明（請求項6に対応）は、システム部とアプリケーシ

ヨンソフトウェア部とを備え、

　　ディジタルインタフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、

　前記システム部は複数種類のタンパ確認関数を有しており、前記アプリケーションソフトウェア部のアプリケーションソフトウェアには所定の種類のタンパ確認関数に対応するタンパコードとその種類情報が埋め込まれており、前記システム部は前記アプリケーションソフトウェア部からタンパコードとその種類情報を読み取り、その種類に対応するタンパ確認関数を用いて、アプリケーションソフトウェアの改竄の有無を判定し、それを利用して、改竄されていることが判明した場合は、その結果を知らせることを特徴とするコンピュータである。

　また第7の本発明（請求項7に対応）は、システム部とアプリケーションソフトウェア部とを備え、

　　ディジタルインタフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、

　前記システム部は、前記アプリケーションソフトウェア部のアプリケーションソフトウェアに関する情報を前記データに埋め込んで前記データをアプリケーション部へ送ることを特徴とするコンピュータである。

　また第8の本発明（請求項8に対応）は、前記アプリケーションソフトウェアに関する情報とは、前記アプリケーションソフトウェアの名前、または前記アプリケーションソフトウェアのバージョン番号、またはタンパコード、またはタンパレジスタンス確認関数の種類情報、または使用者に関する情報を特徴とする第7の発明に記載のコンピュ

ータである。

また第9の本発明（請求項9に対応）は、第1～8の何れかの本発明の全部又は一部の手段の全部又は一部の機能をコンピュータにより実行させるためのプログラム及び／又はデータを担持した媒体であって、コンピュータにより処理可能なことを特徴とする媒体である。

また第10の本発明（請求項10に対応）は、第1～8の何れかの本発明の全部又は一部の手段の全部又は一部の機能をコンピュータにより実行させるためのプログラム及び／又はデータであることを特徴とする情報集合体。

図面の簡単な説明

【図1】

本発明の第1の実施の形態におけるシステム部とアプリケーションソフトウェア部が認証を行い、AVデータはPC内で暗号化される場合のブロック図。

【図2】

本発明の第2の実施の形態におけるCRLを用いて不正なアプリケーションソフトウェアを検出する場合のブロック図。

【図3】

本発明の第3の実施の形態におけるタンパレジスタントの方式を実装した場合のブロック図。

【図4】

本発明の第4の実施の形態における複数種類のタンパ認証関数を実装した場合のブロック図。

【図 5】

本発明の第 5 の実施の形態における著作権主張された A V データに電子透かしを埋め込む場合のブロック図。

【図 6】

本発明の第 6 の実施の形態におけるより確実に著作権主張された A V データの著作権をまもることができる場合のブロック図。

【図 7】

本発明の第 1 の実施の形態におけるアプリケーションソフトウェアのライセンスの種類によって認証が成功するか失敗するかを示した一覧図。

【符号の説明】

- 1 1 3 9 4 D - I F
- 2 伝送認証手段
- 3 アプリ認証関数
- 4 署名メモリ
- 5 データパス
- 6 伝送解読手段
- 7 P C 内用暗号化手段
- 8 アプリ認証手段
- 9 署名生成手段
- 10 データ使用 (デコード表示) 手段
- 11 解読手段
- 12 システム部
- 13 アプリケーションソフトウェア部

- 1 4 C R L メモリ
- 1 5 アプリ用 C R L メモリ
- 1 6 C R L 比較手段
- 1 7 タンパ認証関数
- 1 8、1 9 ソフトチェック手段
- 2 0 バージョン選択手段
- 2 1 タンパ認証関数
- 2 2 署名埋込手段
- 2 3 電子透かし埋込手段

発明を実施するための最良の形態

以下、本発明の実施の形態について図面を参照して説明する。

(実施の形態 1)

第 1 の実施の形態について図 1、図 7 を参照して説明する。本実施の形態では、システム部とアプリケーションソフトウェア部とで認証を行い、また P C に入力された A V データは暗号化されて P C の内部を流通する場合を説明する。図 1 において、P C 2 4 は、システム部 1 2 とアプリケーションソフトウェア部 1 3 から構成される。システム部 1 2 は、P C 2 4 の D - I F ハードウェア内、またはドライバや O S などのシステムソフトウェアである。アプリケーションソフトウェア部 1 3 は、アプリケーションソフトウェアを記録し、またアプリケーションソフトウェアを実行する手段である。

システム部 1 2 は、1 3 9 4 D - I F 1、伝送認証手段 2、アプリ認

証閲数 3、署名メモリ 4、伝送解読手段 6、P C 内用暗号化手段 7 から構成される。

1 3 9 4 D - I F 1 は、シリアルバスインターフェースの標準である I E E E 1 3 9 4 のインターフェースであり、S T B や D - V H S などの外部機器とデータや、コマンドのやり取りを行なうインターフェースである。伝送認証手段 2 は、A V データが著作権主張されている場合、外部機器との間で認証を行い、認証が成功すると伝送解読手段 6 に A V データを復号化するための鍵を渡す手段である。アプリ認証閲数は、1 3 9 4 D - I F 1 を介して入力された A V データが著作権主張されている場合 P C の内部で認証を行う手段である。つまり署名生成手段 9 によって作成された署名を記録した署名メモリ 4 の内容を参照することによってアプリケーションソフトウェア部 1 3 との認証を行い、認証が成功した場合、P C 内用暗号化手段 7 に暗号化の鍵を、アプリ認証手段 8 に復号化のための鍵を渡す手段である。署名メモリ 4 は、署名生成手段 9 で生成された署名を記録するメモリである。伝送解読手段 6 は、外部機器との認証に成功した場合、伝送認証手段 2 から鍵を受け取り、1 3 9 4 D - I F 1 を介して入力される A V データを復号化する手段である。P C 内用暗号化手段 7 は、伝送解読手段 6 で復号化された A V データを、アプリケーションソフトウェア部 1 3 との認証が成功した場合、再び暗号化し、そのデータをアプリケーション部 1 3 に渡す手段である。

アプリケーションソフトウェア部 1 3 は、アプリ認証手段 8 、署名生成手段 9 、データ使用（デコード表示）手段 1 0 、解読手段 1 1 から構成される。

アプリ認証手段8は、システム部12のアプリ認証関数と認証を行う手段である。署名生成手段9は、システム部12と認証を行うために用いるディジタル署名を生成する手段である。データ使用（デコード表示）手段10は、現在起動中のアプリケーションソフトウェアにそのAVデータを利用できるようにする手段である。解読手段11は、システム部12との認証が成功した場合、アプリ認証手段9から復号化のための鍵を入手し、その鍵を用いてPC内用暗号化手段7で暗号化されたAVデータを復号化する手段である。

次にこのような本実施の形態の動作を説明する。

まず著作権情報の表し方について説明する。

STBやVTR等の外部機器からAVデータがPC24に送られてくる際、そのAVデータが著作権主張されている場合がある。すなわち、複製禁止や1回のみ複製を許可するなどの条件が付与されている場合がある。こういった利用許諾を表す信号情報は、ストリーム中に埋め込まれたCGMS (Copy Generation information) を用いて行われている。

CGMSは放送局から送られてくるトランスポートストリームの内部に存在している。CGMSは2ビットのデータであり、CGMSの取りうる値とその意味は次のようになる。

すなわちCGMS=11のときcopy neverを意味し、CGMS=10のときcopy one generationを意味し、CGMS=00のときcopy freeを意味する。またCGMS=01は存在しない。ただしcopy neverは複製禁止のことであ

り、そのAVデータを視聴することだけを許可する。copy one generationは1世代のみ複製を許可するものであり、複製したAVデータは何度でも繰り返して視聴することができるものである。copy freeは自由に複製してよいことを示すものである。CGMSを検出するためにはトランスポートストリームデコーダ回路などが必要になり、ハードウェア構成が複雑になる。

一方、IEEE1394のパケットデータのヘッダ内に利用許諾情報を送るための信号情報（以下EMI（Encryption Mode Indicator）と記す）を付加することによって、トランスポートストリームデコーダ回路などのハードウェアは不要になる。

EMIはCGMSから生成され、次の値をとる。すなわちEMI=11のときcopy neverを意味し、EMI=10のときcopy one generationを意味し、EMI=00のときcopy freeを意味する。またEMI=01はno more copyを意味する。ただしcopy neverは複製禁止のことであり、そのAVデータを視聴することだけを許可する。copy one generationは1世代のみ複製を許可するものであり、複製したAVデータは何度でも繰り返して視聴することができるものである。copy freeは自由に複製してよいことを示すものである。またno more copyはcopy one generationのAVデータを複製した後のAVデータであることを示し、これ以上の複製は不許可を表す。

このようなEMIはIEEE1394では、暗号の方法、認証の方法

を指定するのに用いられる。例えばEMI = 00のcopy freeではAVデータを送る際に暗号化は行われない。またEMI = 10のcopy one generationとEMI = 01のno more copyでは、EMI = 11のcopy neverと暗号化に用いられる鍵や機器の認証方法が異なる。

今、STBからAVデータが送られてきたとする。そうするとSTBから送られてくるAVデータが著作権主張されているかどうかを前述したCGMSやEMIで判断し、著作権主張されている場合は、AVデータの送信元であるSTBと認証を行う。AVデータは暗号化されて送られており、認証に成功すれば、伝送認証手段2はSTBからAVデータを復号化するための鍵を入手する。EMIが11の場合は公開鍵による認証が行われ、またEMIが10か01の場合は共通鍵による認証が行われる。

伝送認証手段とSTBの間で認証に成功すると、次にアプリケーションソフトウェア部13とシステム部12との間で認証を行うようにした。アプリ認証手段8は、署名生成手段9で、現在起動中のアプリケーションソフトウェアのデジタル署名を生成する。署名メモリ4は署名生成手段8で生成されたデジタル署名を記録する。アプリ認証関数3は、署名メモリ4に記録されているデジタル署名をもとにアプリ認証手段8との間で認証を行う。

ただし予めそれぞれのアプリケーションソフトウェアには、著作権主張されたAVデータの利用許諾情報に対応するライセンスを付与しておく。アプリケーションソフトウェア部13とシステム部12との認証に

よって正当なライセンスを有するソフトウェアのみ認証に成功するようとした。具体的には、アプリケーションソフトウェアの機能に応じてライセンスを分類する。AVデータの表示のみ行うソフトウェアに与えるライセンスをライセンスAとし、AVデータを記録するソフトウェアに与えるライセンスをライセンスBとする。さらに著作権主張された内容を厳守するソフトウェアのライセンスをCとする。ライセンスCは、AVデータが複製禁止の場合は、そのAVデータに対しては再生のみ行い、複製をせず、またAVデータが一回限り複製許可の場合は、そのAVデータに対しては一回限り複製を行うようなソフトウェアである。ただしライセンスCの場合、著作権主張されたAVデータの著作権の内容をAVデータとともにアプリケーションソフトウェアに通知する必要があるが、これはEMIまたはCGMSとしてAVデータに組み込んでおけばよい。

現在起動中のアプリケーションソフトウェアのライセンスが、Bであるとする。そして、STBから送られてきたAVデータの利用許諾情報は、EMIが11であるとする。すなわちAVデータの複製は禁止されているとする。この場合、アプリ認証手段8とアプリ認証関数3との間で認証が行われるが、認証は成功しない。また現在起動中のアプリケーションソフトウェアのライセンスが、Aであるとする。この場合このアプリケーションソフトウェアは表示のみを行うソフトウェアであるので、アプリ認証手段8とアプリ認証関数3との間の認証が成功する。さらにAVデータが複製禁止の場合、ライセンスCのアプリケーションソフトウェアである場合は、認証に成功する。AVデータの利用許諾の

種類とアプリケーションソフトウェアのライセンスの種類と認証に成功するか失敗するかの一覧表を図7に示しておく。

アプリケーションソフトウェア部13とシステム部12との認証に成功した場合、伝送解読手段6は、伝送認証手段2から暗号解読用の鍵を受け取って、1394D-IF1を介して送られてくるAVデータを復号化する。次にPC内用暗号化手段7で、このAVデータを再び暗号化する。PC24内では、アプリケーションソフトウェアに使用される直前まで、著作権主張されたAVデータは暗号化されたまま流通する。さらに、データ使用（デコード表示）手段10を構成する解読手段11は、アプリ認証手段8から暗号解読用の鍵を受け取り、AVデータを復号化する。復号化されたAVデータはデータ使用（デコード表示）手段10から、現在起動中のアプリケーションソフトウェアに渡され、処理される。

またアプリケーションソフトウェア部13とシステム部12との認証に失敗した場合、伝送解読手段6がAVデータを復号化したのち、PC内用暗号化手段7で再び暗号化し、データ使用（デコード表示）手段10に送る。認証に失敗したためアプリ認証手段8はアプリ認証関数3から復号化のための鍵を受け取ることはできないので、解読手段11に復号化のための鍵を渡すことは出来ず、従って、解読手段11はAVデータを復号化することは出来ない。このようにライセンスが不適当なアプリケーションソフトウェアの場合、認証に失敗するため、AVデータを復号化して処理することができない。

このように、PC24の内部では、著作権主張されているAVデータ

を暗号化し、さらにシステム部 1 2 とアプリケーションソフトウェア部 1 3との間で認証を行い、ライセンスを受けているアプリケーションソフトウェアを選別することによって、ライセンスを受けていないアプリケーションソフトウェアが A Vデータを受け取っても、データが暗号化されているためにその A Vデータを意味ある物として使用することができず、著作権主張された A Vデータを守ることができる。

なお本発明の再暗号化は、伝送時の暗号化と同じ鍵を用いて暗号化しても構わないし、また伝送時の暗号化とは別の鍵を用いて暗号化しても構わない。さらに伝送時に暗号化されている A Vデータを復号化せず、そのまま P Cの内部に流通させても構わない。また再暗号化の方法は上記の方法以外の独自の方法を用いても構わない。

さらに本実施の形態の P C内用暗号化手段は上述した実施の形態のようにシステム部とアプリケーションソフトウェア部との認証が失敗した場合、暗号化されたデータをデータ使用（デコード表示）手段に送るものに限らず、ブルーバック画面など無効なデータをデータ使用（デコード表示）手段に送るものでも構わない。このようにすることによってより安全に A Vデータの著作権を守ることが出来る。

さらに本発明のシステム部は、1 3 9 4 D – I Fを構成するハードウェアまたはドライバやOSなどのシステムソフトウェアでも実現可能である。要するに、P C内のハードウェアで実現しても構わないし、システムソフトウェアで実現しても構わない。

さらに本実施の形態のライセンスは上述したようにA、B、Cの3種類に分けるものに限らない。4種類や2種類など、要するに、A Vデータ

タの著作権情報の種類に対応する分け方でありさえすればよい。

さらに本実施の形態では外部機器としてSTBを例にあげて、STBから著作権主張されたAVデータをPCが受けとるとして説明したが、これに限らず、外部機器としてDVC、DVHS、HDD、DVD-RAM、放送受信機など、要するに著作権主張されたAVデータを送ることのできる機器であればなんでもよい。

さらに、本実施の形態ではIEEE1394を例にあげて説明したが、これに限らず、著作権主張されたAVデータをその著作権情報とともに伝送する仕組みのあるネットワークであればなんでも良い。

さらに本実施の形態のAVデータは上述したように映像音声データに限らず、著作権主張されたプログラムや文書など、要するに著作権が主張されているデータでありさえすればよい。

さらに本実施の形態のPCは本発明のコンピュータの例である。

(実施の形態2)

次に第2の実施の形態について図2を参照して説明する。

本実施の形態では、システム部とアプリケーションソフトウェア部とで認証を行う前に不正なまたは正当なアプリケーションソフトウェアを示す管理基準（以下CRLと呼ぶ）によってアプリケーションソフトウェアを判定しておく場合を説明する。

第1の実施の形態との相違点は、システム部12がCRLメモリ14、アプリ用CRLメモリ15、CRL比較手段16を有する点である。以下第1の実施の形態との相違点を中心に説明する。

CRLメモリ14は、不正なまたは正当な機器を示す管理基準を記憶

するメモリである。またアプリ用CRLメモリ15は、不正なまたは正当なアプリケーションソフトウェアを示す管理基準を記憶する手段である。CRL比較手段16はCRLによってアプリケーションソフトウェアが不正か正当かを判断する手段である。

次にこのような本実施の形態の動作を説明する。

本実施の形態でもSTBからAVデータが送られてくるとし、そのAVデータは著作権主張されているとする。まず第1に伝送解読手段6とSTBの間で認証を行う前にSTBのCRLメモリに記憶されているCRLを用いてPC24が正当な機器か不正な機器かの判定がなされる。正当な機器と判定されれば、伝送認証手段2がSTBとの認証を行う。不正な機器と判定されればSTBは認証を行わず、暗号化されているAVデータを復号化する鍵をPC24に渡さない。

今、PC24はSTBによって正当な機器と判定されたとする。そうすると伝送認証手段2が1394D-I/F1を介してSTBと認証を行う。認証が成功すれば、STBはAVデータを復号化するための鍵を1394D-I/F1を介して、伝送認証手段2に渡す。

次に署名生成手段9は、現在起動しているアプリケーションソフトウェアのデジタル署名を作成し、署名メモリ4が記憶する。CRL比較手段16は署名メモリ4に記憶されているデジタル署名の内容と、アプリ用CRLメモリ15の内容を比較し、現在起動中のアプリケーションソフトウェアが不正なソフトウェアか正当なソフトウェアかどうかを判定する。不正なソフトウェアである場合は、アプリケーションソフトウェア部13とシステム部12との認証を行わない。また正当なソフト

ウェアである場合は、次にアプリケーションソフトウェア部13とシステム部12との間で認証を行うようにした。ただしアプリケーションソフトウェアには第1の実施の形態と同様のライセンスが付与されているとする。

ここで、アプリ用CRLメモリ15は、PC24内のOSやドライバ等のメモリであって、独自に予め作成したCRLを記憶しておいてもよいし、IEEE1394から送られてくるCRLを流用してもよい。このCRLは一般に固定されたものでは無く、状況に応じて更新することが出来る。例えば機器やアプリケーションが著作権を侵害するように改変され流通した場合に、それらを特定して認証を失敗させるよう、CRLを更新することが可能である。

アプリケーションソフトウェア部13とシステム部12との認証に成功した場合、伝送解読手段6は、伝送認証手段2から暗号解読用の鍵を受け取って、1394D-IFを介して送られてくるAVデータを復号化する。次にPC内用暗号化手段7で、このAVデータを再び暗号化する。PC24内では、アプリケーションソフトウェアに使用される直前まで、著作権主張されたAVデータは暗号化されたまま流通する。さらに、データ使用（デコード表示）手段10を構成する解読手段11は、アプリ認証手段8から暗号解読用の鍵を受け取り、AVデータを復号化する。復号化されたAVデータはデータ使用（デコード表示）手段10から、現在起動中のアプリケーションソフトウェアに渡され、処理される。

またアプリケーションソフトウェア部13とシステム部12との認証

に失敗した場合、伝送解読手段 6 が A V データを復号化したのち、P C 内用暗号化手段 7 で再び暗号化し、データ使用（デコード表示）手段 1 0 に送る。認証に失敗したためアプリ認証手段 8 は復号化のための鍵を解読手段 1 1 に渡すことは出来ず、従って、解読手段 1 1 は A V データを復号化することは出来ない。従ってライセンスが不適当なアプリケーションソフトウェアの場合、認証に失敗するため、A V データを処理することができない。

あるいは、アプリ用 C R L メモリ 1 5 から、破られ無効になったタンパレジスタンス方式のバージョン情報を入手し、アプリケーションが無効となったバージョンしか持たない場合には、アプリ認証関数 3 に A V データを復号するための鍵を渡さず、システム部 1 2 とアプリケーションソフトウェア部 1 3 との認証も行わない。

このように、アプリケーションソフトウェア部とシステム部で認証する前に C R L を用いて現在起動中のアプリケーションソフトウェアが不正か正当かを判断することによって、著作権主張された A V データに対して、不正な動作を行うアプリケーションソフトウェアを予め排斥することができる。

なお本発明の再暗号化は、伝送時の暗号化と同じ鍵を用いて暗号化しても構わないし、また伝送時の暗号化とは別の鍵を用いて暗号化しても構わない。さらに伝送時に暗号化されている A V データを復号化せず、そのまま P C の内部に流通させても構わない。また再暗号化の方法は上記の方法以外の独自の方法を用いても構わない。

さらに本実施の形態の P C 内用暗号化手段は上述した実施の形態のよ

うにシステム部とアプリケーションソフトウェア部との認証が失敗した場合、暗号化されたデータをデータ使用（デコード表示）手段に送るものに限らず、ブルーバック画面など無効なデータをデータ使用（デコード表示）手段に送るものでも構わない。このようにすることによってより安全にAVデータの著作権を守ることが出来る。

さらに本発明のシステム部は、1394D-IFを構成するハードウェアまたはドライバやOSなどのシステムソフトウェアでも実現可能である。要するに、PC内のハードウェアで実現しても構わないし、システムソフトウェアで実現しても構わない。

さらに本実施の形態では外部機器としてSTBを例にあげて、STBから著作権主張されたAVデータをPCが受けとるとして説明したが、これに限らず、外部機器としてDVC、DVHS、HDD、DVD-RAM、放送受信機など、要するに著作権主張されたAVデータを送ることのできる機器であればなんでもよい。

さらに、本実施の形態ではIEEE1394を例にあげて説明したが、これに限らず、著作権主張されたAVデータをその著作権情報とともに伝送する仕組みのあるネットワークであればなんでも良い。

さらに本実施の形態のAVデータは上述したように映像音声データに限らず、著作権主張されたプログラムや文書など、要するに著作権が主張されているデータでありさえすればよい。

さらに本実施の形態のPCは本発明のコンピュータの例である。

（実施の形態3）

次に第3の実施の形態について図3を参照して説明する。

本実施の形態ではタンパ認証関数を用いてアプリケーションソフトウェアが不正に改竄されているかどうかを判定する場合を説明する。

第1の実施の形態との相違点は、システム部12がタンパ認証関数17を有し、またアプリケーションソフトウェア部13がソフトチェック手段18を有する点である。

タンパ認証関数17は、アプリケーションソフトウェアから発生するタンパコードを検証し、アプリケーションソフトウェアが改竄されていないかどうかの確認を行う手段である。ソフトチェック手段18は、現在起動しているアプリケーションをチェックし、タンパコードを発生させる手段である。

次にこのような本実施の形態の動作を説明する。

上述したようにタンパコードを発生するタンパレジスタンツソフトウェアとは、内部解析や改変に対して耐性を備えているソフトウェアである。すなわち著作権主張されたAVデータを不正に利用しようとする悪意を持つユーザの攻撃があっても、防御できるようにしたソフトウェアである。タンパレジスタンツソフトウェアはタンパコードと呼ばれるコードを発生する。ソフトチェック手段18はプログラムを調べて改竄の有無を検証し、さらに実行環境を調べてデータ経路での傍受の有無やプログラムの実行を監視する第3者の存在などを検証する。タンパコードとはこの検証の結果か、または中間結果を表すデータである。このコードを検証することによって、タンパレジスタンツソフトウェアが改竄されていないかどうかを確認することができる。つまり本実施の形態ではアプリケーションソフトウェアはタンパレジスタンツの方式を実装して

いるものとする。

第1の実施の形態と同様にSTBと伝送認証手段2との間で認証が行われ、認証が成功したものとする。そうすると、ソフトチェック手段18は、現在起動中のアプリケーションソフトウェアをチェックし、タンパコードを発生させる。発生したタンパコードは、アプリ認証手段に渡され、さらに署名生成手段9で、デジタル署名に書き込まれ、このデジタル署名は署名メモリ4に記憶される。タンパ認証関数17は、署名メモリ4に記憶されているデジタル署名を参照し、現在起動しているアプリケーションソフトウェアのタンパコードを取り出し、検証する。その結果現在起動しているアプリケーションが不正に改竄されていないか、データの傍受やプログラムの実行の監視が行われていないかどうかの判定結果をアプリ認証関数3に通知する。以下、簡単のため、データの傍受やプログラムの実行の監視が行われていないかどうかの判定もアプリケーションが不正に改竄されて居ないかの判定に含まれることとして説明する。アプリ認証関数3はアプリケーションソフトウェアが不正に改竄されている場合、アプリ認証手段8にAVデータを復号化するための鍵を渡さず、システム部12とアプリケーションソフトウェア部13との認証も行わない。また不正に改竄されていない場合は、アプリ認証関数3とアプリ認証手段8は、署名メモリ4に記録されているデジタル署名をもとに認証を行う。ただし第1の実施の形態と同様にアプリケーションソフトウェアにはライセンスが付与されている。認証が成功すると、アプリ認証関数3はAVデータを復号化するための鍵をアプリ認証手段8に渡す。

アプリケーションソフトウェア部 13 とシステム部 12 との認証に成功した場合、伝送解読手段 6 は、伝送認証手段 2 から暗号解読用の鍵を受け取って、1394D-IF1 を介して送られてくる AV データを復号化する。次に PC 内用暗号化手段 7 で、この AV データを再び暗号化する。PC 24 内では、アプリケーションソフトウェアに使用される直前まで、著作権主張された AV データは暗号化されたまま流通する。さらに、データ使用（デコード表示）手段 10 を構成する解読手段 11 は、アプリ認証手段 8 から復号化用の鍵を受け取り、AV データを復号化する。復号化された AV データはデータ使用（デコード表示）手段 10 から、現在起動中のアプリケーションソフトウェアに渡され、処理される。

またアプリケーションソフトウェア部 13 とシステム部 12 との認証に失敗した場合、伝送解読手段 6 が AV データを復号化したのち、PC 内用暗号化手段 7 で再び暗号化し、データ使用（デコード表示）手段 10 に送る。認証に失敗したためアプリ認証手段 8 は復号化のための鍵を解読手段 11 に渡すことは出来ないので、解読手段 11 は AV データを復号化することは出来ない。従ってライセンスが不適当なアプリケーションソフトウェアの場合、認証に失敗するため、AV データを処理することができない。

このようにアプリケーションソフトウェアにタンパレジストントの方式を実装し、さらにアプリケーションソフトウェアが不正に改竄されていないかどうかを確認する機能を付加することによってより確実に AV データの著作権を守ることができる。

なお本発明の再暗号化は、伝送時の暗号化と同じ鍵を用いて暗号化し

ても構わないし、また伝送時の暗号化とは別の鍵を用いて暗号化しても構わない。さらに伝送時に暗号化されているAVデータを復号化せず、そのままPCの内部に流通させても構わない。また再暗号化の方法は上記の方法以外の独自の方法を用いても構わない。

さらに本実施の形態のPC内用暗号化手段は上述した実施の形態のようにシステム部とアプリケーションソフトウェア部との認証が失敗した場合、暗号化されたデータをデータ使用（デコード表示）手段に送るものに限らず、ブルーバック画面など無効なデータをデータ使用（デコード表示）手段に送るものでも構わない。このようにすることによってより安全にAVデータの著作権を守ることが出来る。

さらに本発明のシステム部は、1394D-IFを構成するハードウェアまたはドライバやOSなどのシステムソフトウェアでも実現可能である。要するに、PC内のハードウェアで実現しても構わないし、システムソフトウェアで実現しても構わない。

さらに本実施の形態では外部機器としてSTBを例にあげて、STBから著作権主張されたAVデータをPCが受けとるとして説明したが、これに限らず、外部機器としてDVC、DVHS、HDD、DVD-RAM、放送受信機など、要するに著作権主張されたAVデータを送ることのできる機器であればなんでもよい。

さらに、本実施の形態ではIEEE1394を例にあげて説明したが、これに限らず、著作権主張されたAVデータをその著作権情報とともに伝送する仕組みのあるネットワークであればなんでも良い。

さらに本実施の形態のAVデータは上述したように映像音声データに

限らず、著作権主張されたプログラムや文書など、要するに著作権が主張されているデータでありさえすればよい。

さらに本発明のタンパコード及びタンパレジスタンス確認関数は、タンパレジスタントの方式によらず、任意のタンパレジスタントの方式を用いることができる。

さらに本実施の形態のPCは本発明のコンピュータの例であり、本実施の形態のタンパ認証関数は本発明のタンパレジスタンス確認関数の例である。

(実施の形態4)

次に第4の実施の形態について図4を参照して説明する。

本実施の形態ではタンパ認証関数を用いてアプリケーションソフトウェアが不正に改竄されているかどうかを判定する場合を説明する。

第3の実施の形態との相違点は、システム部12が複数種類のタンパ認証関数21を有し、またバージョン選択手段20を有し、またアプリケーションソフトウェア部13のソフトチェック手段19がタンパコードに加えてアプリケーションソフトウェアに実装しているタンパレジスタントの方式の種類情報を発生する点である。

バージョン選択手段20は、署名メモリ4に記録されているディジタル署名をもとにタンパレジスタントの方式の種類に対応するタンパ認証関数を選択する手段である。

次にこのような本実施の形態の動作を説明する。

第3の実施の形態と同様、アプリケーションソフトウェアはタンパレジスタントの方式を実装しているとする。第3の実施の形態と同様にS

T B と伝送認証手段 2 とで認証が行われ、認証が成功したものとする。そうすると、ソフトチェック手段 19 は、現在起動中のアプリケーションソフトウェアをチェックし、タンパコードと実装しているタンパレジスタンスト的方式の種類情報を発生させる。発生したタンパコードと種類情報は、アプリ認証手段 8 に渡され、さらに署名生成手段 9 で、デジタル署名に書き込まれ、このデジタル署名は署名メモリ 4 に記憶される。バージョン選択手段 20 は、署名メモリ 4 に記憶されているタンパレジスタンスト的方式の種類情報を参照し、使用するタンパ認証関数を選択する。この際、バージョン選択手段 20 は、図では省略するがタンパバージョンに関する独自の C R L メモリを備えているものとし、この C R L メモリを利用する事で、既に破る方法が知られているタンパレジスタンスチェック手段 19 を選択しないという動作を行う。選択されたタンパ認証関数 21 は、署名メモリ 4 に記憶されているデジタル署名を参照し、現在起動しているアプリケーションソフトウェアのタンパコードを取り出し、検証する。その結果現在起動しているアプリケーションソフトウェアが不正に改竄されていないかどうかの判定結果をアプリ認証関数 3 に通知する。アプリ認証関数 3 はアプリケーションソフトウェアが不正に改竄されている場合、アプリ認証手段 8 に A V データを復号化するための鍵を渡さず、システム部 12 とアプリケーションソフトウェア部 13 との認証も行わない。また不正に改竄されていない場合は、アプリ認証関数 3 とアプリ認証手段 8 は、署名メモリ 4 に記録されているデジタル署名をもとに認証を行う。ただし第 1 の実施の形態と同様にアプリケーションソフトウェアにはライセンスが付与されている。認

証が成功すると、アプリ認証関数3はAVデータを復号化するための鍵をアプリ認証手段8に渡す。

アプリケーションソフトウェア部13とシステム部12との認証に成功した場合、伝送解読手段6は、伝送認証手段2から暗号解読用の鍵を受け取って、1394D-IF1を介して送られてくるAVデータを復号化する。次にPC内用暗号化手段7で、このAVデータを再び暗号化する。PC24内では、アプリケーションソフトウェアに使用される直前まで、著作権主張されたAVデータは暗号化されたまま流通する。さらに、データ使用（デコード表示）手段10を構成する解読手段11は、アプリ認証手段8から復号化用の鍵を受け取り、AVデータを復号化する。復号化されたAVデータはデータ使用（デコード表示）手段10から、現在起動中のアプリケーションソフトウェアに渡され、処理される。

またアプリケーションソフトウェア部13とシステム部12との認証に失敗した場合、伝送解読手段6がAVデータを復号化したのち、PC内用暗号化手段7で再び暗号化し、データ使用（デコード表示）手段10に送る。認証に失敗したためアプリ認証手段8は復号化のための鍵を解読手段11に渡すことは出来ず、解読手段11はAVデータを復号化することは出来ない。従ってライセンスが不適当なアプリケーションソフトウェアの場合、認証に失敗するため、AVデータを処理することができない。

このようにアプリケーションソフトウェアにタンパレジスタン트の方式を実装するのみならず、複数個のタンパレジスタント認証関数をシステム部に実装することにより、アプリケーションソフトウェアのタンパ

レジスタントの方式が例え破られたとしても、システム部はタンパレジスタンント認証関数を別の種類に切り替えるだけですみ、OSのバージョンアップなどを行う必要がないので、タンパレジスタンントの方式が破られたことによる被害を最小限に抑えることができる。

なお本発明の再暗号化は、伝送時の暗号化と同じ鍵を用いて暗号化しても構わないし、また伝送時の暗号化とは別の鍵を用いて暗号化しても構わない。さらに伝送時に暗号化されているAVデータを復号化せず、そのままPCの内部に流通させても構わない。また再暗号化の方法は上記の方法以外の独自の方法を用いても構わない。

さらに本実施の形態のPC内用暗号化手段は上述した実施の形態のようにシステム部とアプリケーションソフトウェア部との認証が失敗した場合、暗号化されたデータをデータ使用（デコード表示）手段に送るものに限らず、ブルーバック画面など無効なデータをデータ使用（デコード表示）手段に送るものでも構わない。このようにすることによってより安全にAVデータの著作権を守ることが出来る。

さらに本発明のシステム部は、1394D-IFを構成するハードウェアまたはドライバやOSなどのシステムソフトウェアでも実現可能である。要するに、PC内のハードウェアで実現しても構わないし、システムソフトウェアで実現しても構わない。

さらに本実施の形態では外部機器としてSTBを例にあげて、STBから著作権主張されたAVデータをPCが受けとるとして説明したが、これに限らず、外部機器としてDVC、DVHS、HDD、DVD-RAM、放送受信機など、要するに著作権主張されたAVデータを送るこ

とのできる機器であればなんでもよい。

さらに、本実施の形態では I E E E 1 3 9 4 を例にあげて説明したが、これに限らず、著作権主張された A V データをその著作権情報とともに伝送する仕組みのあるネットワークであればなんでも良い。

さらに本実施の形態の A V データは上述したように映像音声データに限らず、著作権主張されたプログラムや文書など、要するに著作権が主張されているデータでありさえすればよい。

さらに本発明のタンパコード及びタンパレジスタンス確認関数は、タンパレジスタンントの方式によらず、任意のタンパレジスタンントの方式を用いることができる。

さらに本実施の形態の P C は本発明のコンピュータの例であり、本実施の形態のタンパ認証関数は本発明のタンパレジスタンス確認関数の例である。

(実施の形態 5)

次に第 5 の実施の形態について図 5 を参照して説明する。

本実施の形態では、 A V データを処理するアプリケーションソフトウェアに関する情報を電子透かしによって A V データに埋め込む場合を説明する。

ここでいう電子透かしとは署名などのデータを A V データに改変が困難なように織り込むための技術を指すこととし、アナログ的なデータ重畳に基づくものか、デジタル的に暗号技術に基づくものかなどは問わない。

第 1 、 2 の実施の形態との相違点は、システム部に署名埋め込み手段

22、電子透かし埋め込み手段23を有している点である。

署名埋め込み手段22は、署名メモリ4に記録されているデジタル署名の内容を参照し、電子透かし埋め込み手段23で必要な情報を選別し、書式を整えるなどの電子透かし埋め込み手段23の前処理を行う手段である。電子透かし埋め込み手段23は、署名埋め込み手段22で整えられた書式で、AVデータに電子透かしによるデータの埋め込みを行う手段である。

本実施の形態のうち伝送認証手段2、アプリ認証関数3、署名メモリ4、アプリ認証手段8、署名生成手段9、伝送解読手段6、PC内用暗号化手段7、データ使用（デコード表示）手段10、解読手段11は、第1の実施の形態と同じである。またCRLメモリ14、アプリ用CRLメモリ15、CRL比較手段16は、第2の実施の形態と同じである。

次にこのような本実施の形態の動作を説明する。

外部の機器、例えばSTBと伝送認証手段2と認証を行い成功したとする。さらにアプリ認証手段8とアプリ認証関数3の間での認証も成功したとする。そうすると1394D-IF1から入力された暗号化されているAVデータは伝送解読手段6で復号化される。署名埋め込み手段22は、署名メモリ4よりアプリケーションソフトウェアの情報を含んだデジタル署名を取り出し、内容を選別する。選別される内容は、アプリケーションソフトウェアのソフト名、アプリケーションソフトウェアのバージョン番号、使用者に関する情報、AVデータ自身の情報である。署名埋め込み手段22は、これらの情報に書式を整える等の前処理を施し、電子透かし埋め込み手段23に送る。電子透かし埋め込み手段

23は、復号化されたAVデータ自身にこれらの情報の電子透かしを作成する。電子透かしを作成されたAVデータはPC内用暗号化手段7で再び暗号化され、データ使用（デコード表示）手段10に渡される。解読手段11がAVデータを復号化し、データ使用（デコード表示手段）10が現在起動中のアプリケーションソフトウェアにそのAVデータを渡す。AVデータを受け取ったアプリケーションソフトウェアは表示、記録、再生などの処理を行う。

ここで、アプリケーションソフトウェアが電子透かしを施されたAVデータを不正に記録し、PC24の外部に配布したとする。この不正に配布されたAVデータは、AVデータのCGMSやEMIが不正なアプリケーションによって書き替えられてしまったとする。そうすると、正当な機器でも記録できるようになり、このAVデータは様々な機器に流出していく。このように不正に流出していったAVデータをチェックする管理機関がこのAVデータ入手すれば、AVデータに埋め込まれた電子透かしを参照することにより以下のことがわかる。すなわち、AVデータの情報からそのAVデータが記録禁止等であることがわかり、またそのAVデータを不正に複製、配布したアプリケーションソフトウェアに関する情報がわかり、出所のアプリケーションソフトウェアを特定することができる。

このように本発明では不正配布の出所に関する情報を特定できるが、さらに本発明のコンピュータは、CRLを更新する手段を備えているため、前記の出所に関する情報に基づいてCRLを更新することで、不正配布を行ったアプリケーションを、以後AVデータの利用から排除し、

そのことにより以後の不正利用を防止する具体的手段を提供する。このように電子透かしを用いることにより不正な複製の出所を特定し、容易に不正なアプリケーションソフトウェアを特定することができる。

なお、電子透かしの方式は本実施の形態で用いたものに限らず、AVデータ内に正しく前述の情報を埋め込むことが出来、所定の形式によりデコード前あるいはデコード後にAVデータから前述の情報が正しく抽出出来るものであればどのような方式のものを用いても構わない。

このように、AVデータに電子透かしを埋め込むことによって、不正なアプリケーションソフトウェアを容易に特定し、排斥することができるようになる。

(実施の形態 6)

次に第6の実施の形態について図6を参照して説明する。

本実施の形態のPCは以上第1～第5の実施の形態で説明したすべてのPCの機能を備えるものである。

伝送認証手段2、アプリ認証関数3、署名メモリ4、アプリ認証手段8、署名生成手段9、伝送解読手段6、PC内用暗号化手段7、データ使用（デコード表示）手段10、解読手段11は第1の実施の形態で説明したものと同様である。また、CRLメモリ14、アプリ用CRLメモリ15、CRL比較手段16は第2の実施の形態で説明したのと同様である。またバージョン選択手段20、タンパ認証関数21は、第4の実施の形態で説明したのと同様である。また署名埋め込み手段22、電子透かし埋め込み手段23は第5の実施の形態で説明したのと同様である。

このように構成することにより、第1～第5の各実施の形態で説明した機能が全て含まれているので、タンパレジスタントの採用によるソフトウェアの信頼性のチェックと、電子透かしによる確実な不正検出方式と、不正検出した際の再発防止手段を備えることで、著作権主張されたAVデータの不正利用防止が確実に行え、かつタンパレジスタント方式に対するバージョンの採用により不正利用の際の2次被害を最小限に限定出来るという効果が得られる。

なお、本発明は、上記実施の形態の何れかに記載の発明の全部又は一部の手段の全部又は一部の機能をコンピュータにより実行させるためのプログラム及び／又はデータを記録したプログラム記録媒体であって、コンピュータにより読み取り可能であり、読み取られた前記プログラム及び／又はデータが前記コンピュータと協動して前記機能を実行するプログラム記録媒体であっても良い。

なお、データとは、データ構造、データフォーマット、データの種類などを含む。

また、媒体とは、ROM等の記録媒体、インターネット等の伝送媒体、光・電波・音波等の伝送媒体を含む。

また、担持した媒体とは、例えば、プログラム及び／又はデータを記録した記録媒体、やプログラム及び／又はデータを伝送する伝送媒体等をふくむ。

また、コンピュータにより処理可能とは、例えば、ROMなどの記録媒体の場合であれば、コンピュータにより読みとり可能であることであり、伝送媒体の場合であれば、伝送対象となるプログラム及び／又はデ

ータが伝送の結果として、コンピュータにより取り扱えることであることを含む。

また、情報集合体とは、例えば、プログラム及び／又はデータ等のソフトウェアを含むものである。

産業上の利用可能性

以上説明したところから明らかなように、本発明は、著作権主張されたデータに対してはアプリケーションソフトウェアが著作権を守り、アプリケーションソフトウェアの不正な改竄に対抗することが出来、不正なアプリケーションソフトウェアに対して、そのアプリケーションソフトウェアを確認し、排斥することが出来、不正な流出をコストをかけずに排除する事が出来るコンピュータ及びプログラム記録媒体を提供することが出来る。

請　　求　　の　　範　　囲

1. システム部とアプリケーションソフトウェア部とを備え、ディジタルインターフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、前記システム部は、前記アプリケーションソフトウェア部が著作権を守る上において正当なアプリケーションソフトウェアであると判定し、正当なものである場合は、暗号化データの鍵をアプリケーションソフトウェア部に渡すことを特徴とするコンピュータ。
2. 前記システム部における判定は、前記システム部とアプリケーションソフトウェア部との間における認証で行われることを特徴とする請求項1記載のコンピュータ。
3. 前記システム部における判定は、不正なまたは正当なアプリケーションソフトウェアが載っているCRL (C e r t i f i c a t i o n R e v o c a t i o n L i s t) で行うことを特徴とする請求項1記載のコンピュータ。
4. 前記システム部は前記暗号化された鍵を外部との認証結果により得て、前記暗号化されたデータを復号し、再度その鍵または別の鍵で復号化されたデータを再暗号化することを特徴とする請求項1～3のいずれかに記載のコンピュータ。
5. 前記システム部はタンパ確認関数を有しており、前記アプリケーションソフトウェア部のアプリケーションソフトウェアにタンパコードが埋め込まれており、前記システム部は前記アプリケーションソフトウェア部からタンパコードを読みとり、タンパ確認関数を用いて、アブ

リケーションソフトウェアの改竄の有無を判定し、それを利用して、改竄されていることが判明した場合は、その結果を知らせることを特徴とする請求項1～4のいずれかに記載のコンピュータ。

6. システム部とアプリケーションソフトウェア部とを備え、ディジタルインタフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、

前記システム部は複数種類のタンパ確認関数を有しており、前記アプリケーションソフトウェア部のアプリケーションソフトウェアには所定の種類のタンパ確認関数に対応するタンパコードとその種類情報が埋め込まれており、前記システム部は前記アプリケーションソフトウェア部からタンパコードとその種類情報を読み取り、その種類に対応するタンパ確認関数を用いて、アプリケーションソフトウェアの改竄の有無を判定し、それを利用して、改竄されていることが判明した場合は、その結果を知らせることを特徴とするコンピュータ。

7. システム部とアプリケーションソフトウェア部とを備え、ディジタルインタフェースから著作権主張された暗号化データを取り込み、処理するコンピュータにおいて、

前記システム部は、前記アプリケーションソフトウェア部のアプリケーションソフトウェアに関する情報を前記データに埋め込んで前記データをアプリケーション部へ送ることを特徴とするコンピュータ。

8. 前記アプリケーションソフトウェアに関する情報とは、前記アプリケーションソフトウェアの名前、または前記アプリケーションソフトウェアのバージョン番号、またはタンパコード、またはタンパレジス

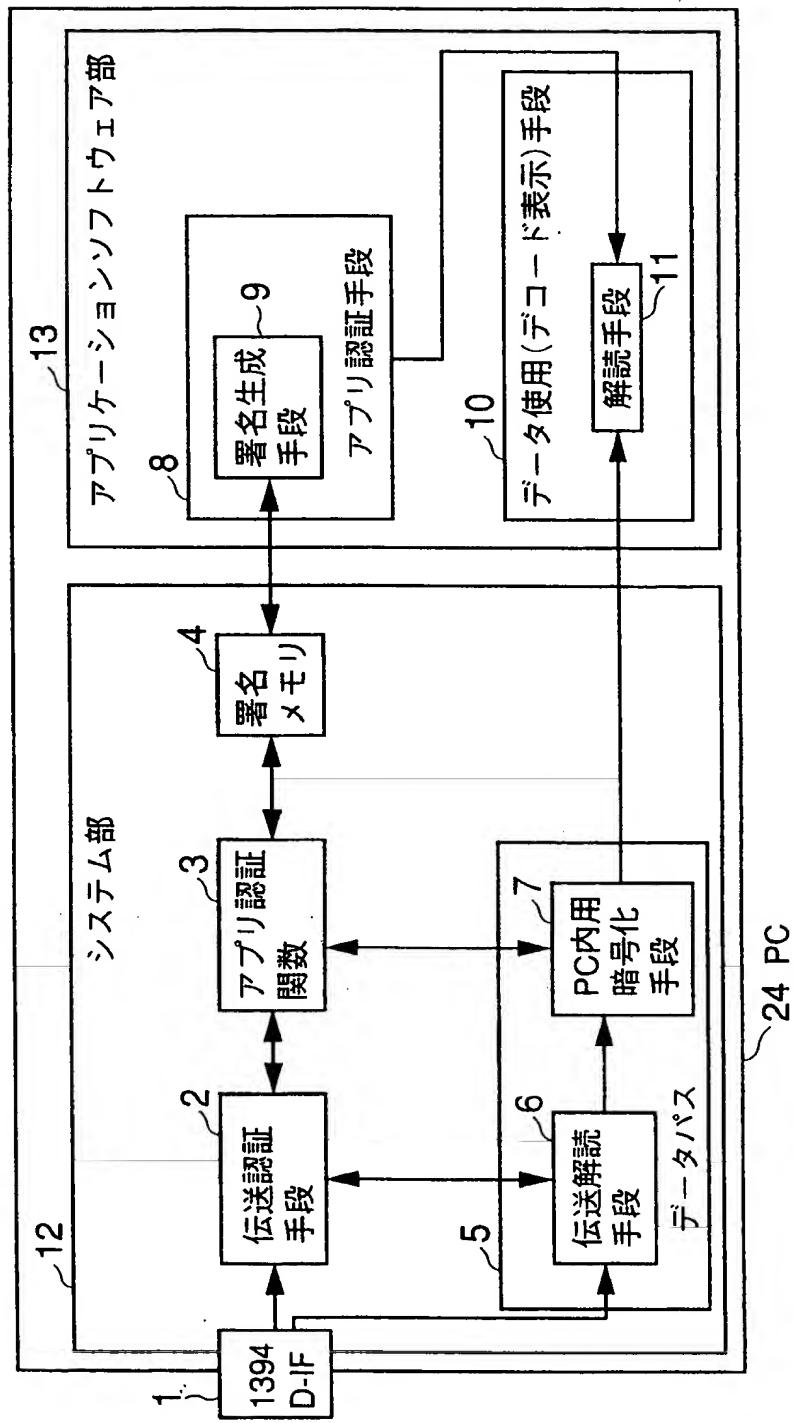
タンス確認関数の種類情報、または使用者に関する情報であることを特徴とする請求項 7 記載のコンピュータ。

9. 請求項 1 ~ 8 の何れかに記載の本発明の全部又は一部の手段の全部又は一部の機能をコンピュータにより実行させるためのプログラム及び／又はデータを担持した媒体であって、コンピュータにより処理可能なことを特徴とする媒体。

10. 請求項 1 ~ 8 の何れかに記載の本発明の全部又は一部の手段の全部又は一部の機能をコンピュータにより実行させるためのプログラム及び／又はデータであることを特徴とする情報集合体。

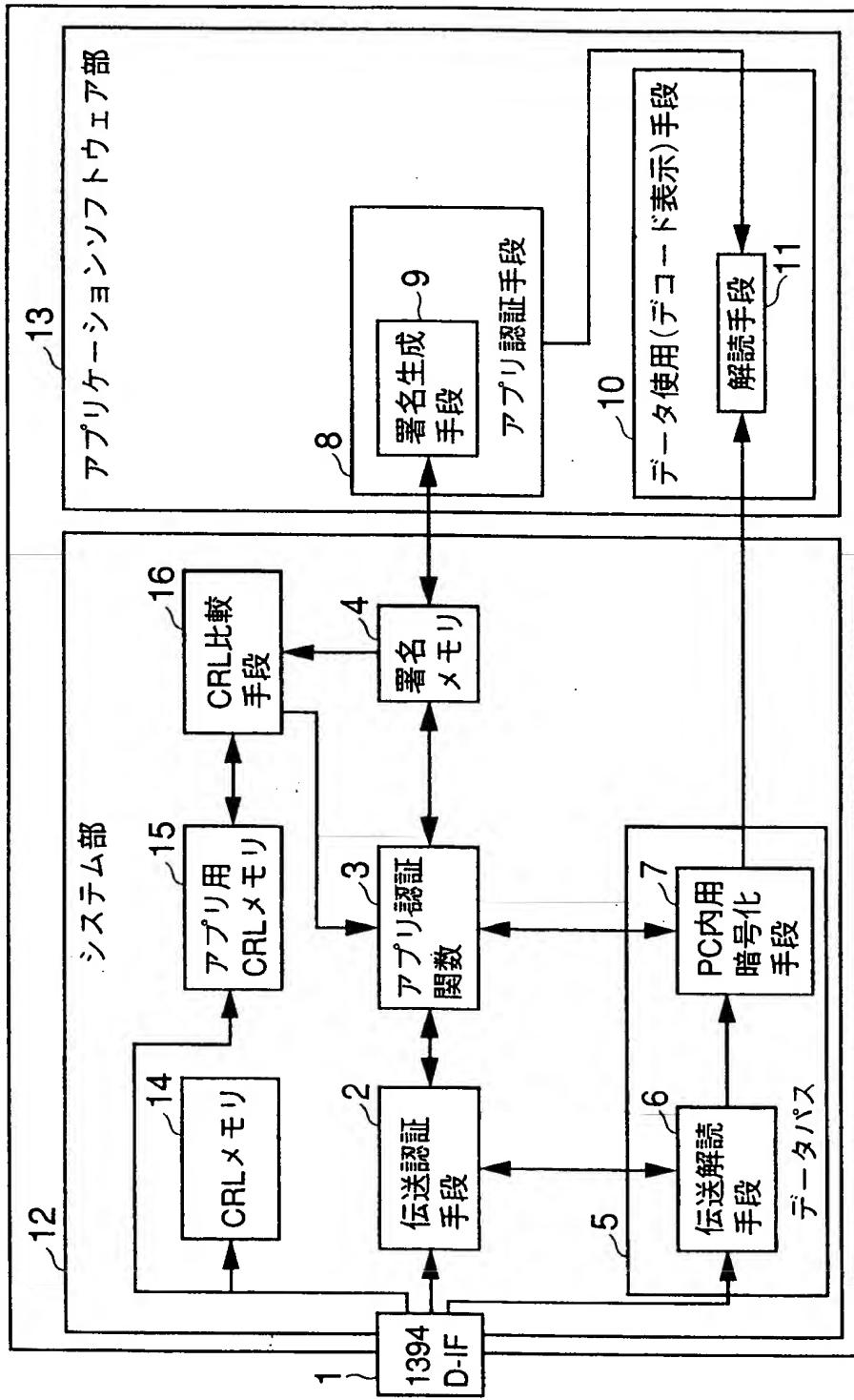
THIS PAGE BLANK (USPTO)

第 1 図



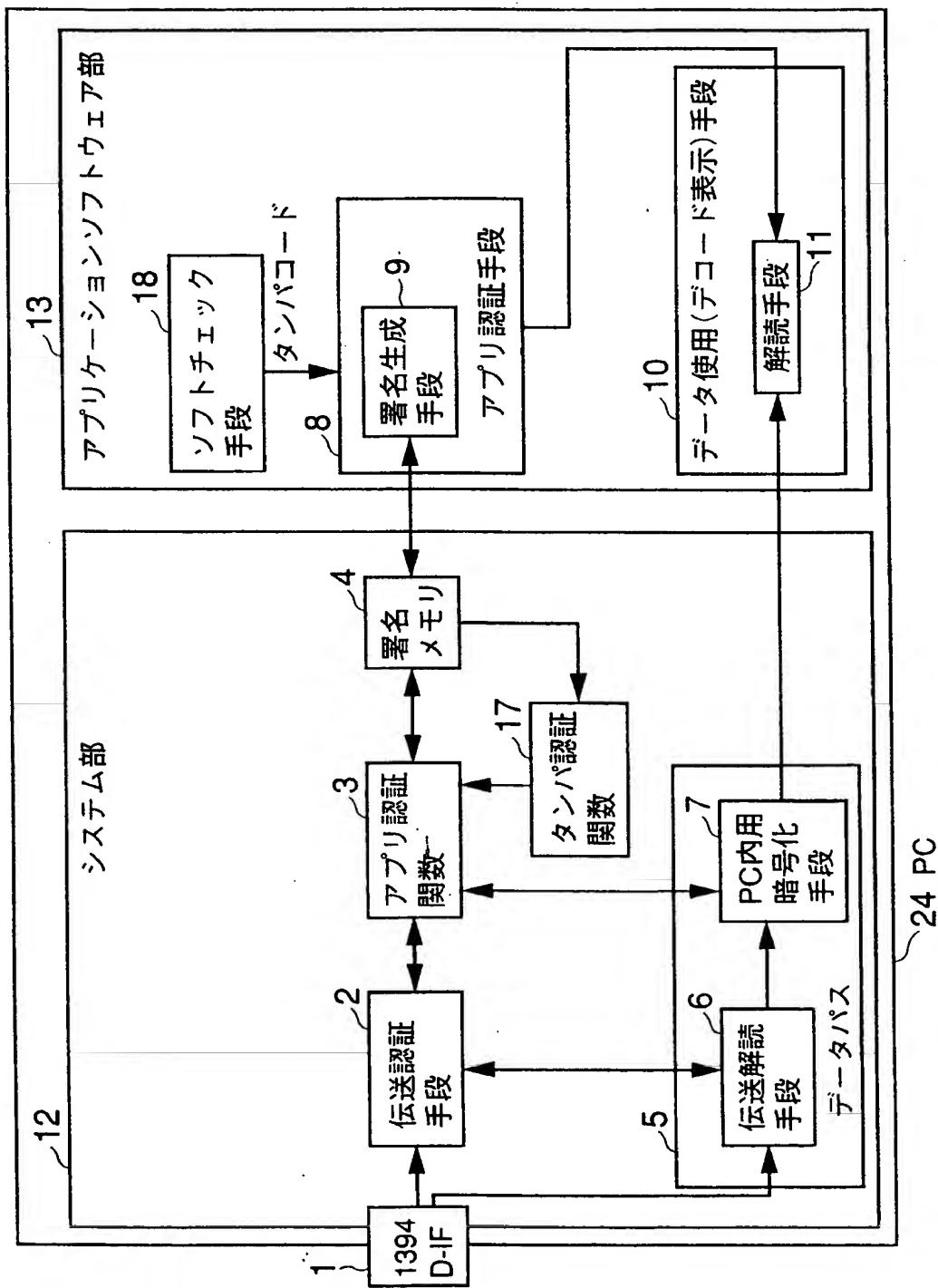
THIS PAGE BLANK (081)

第 2 図



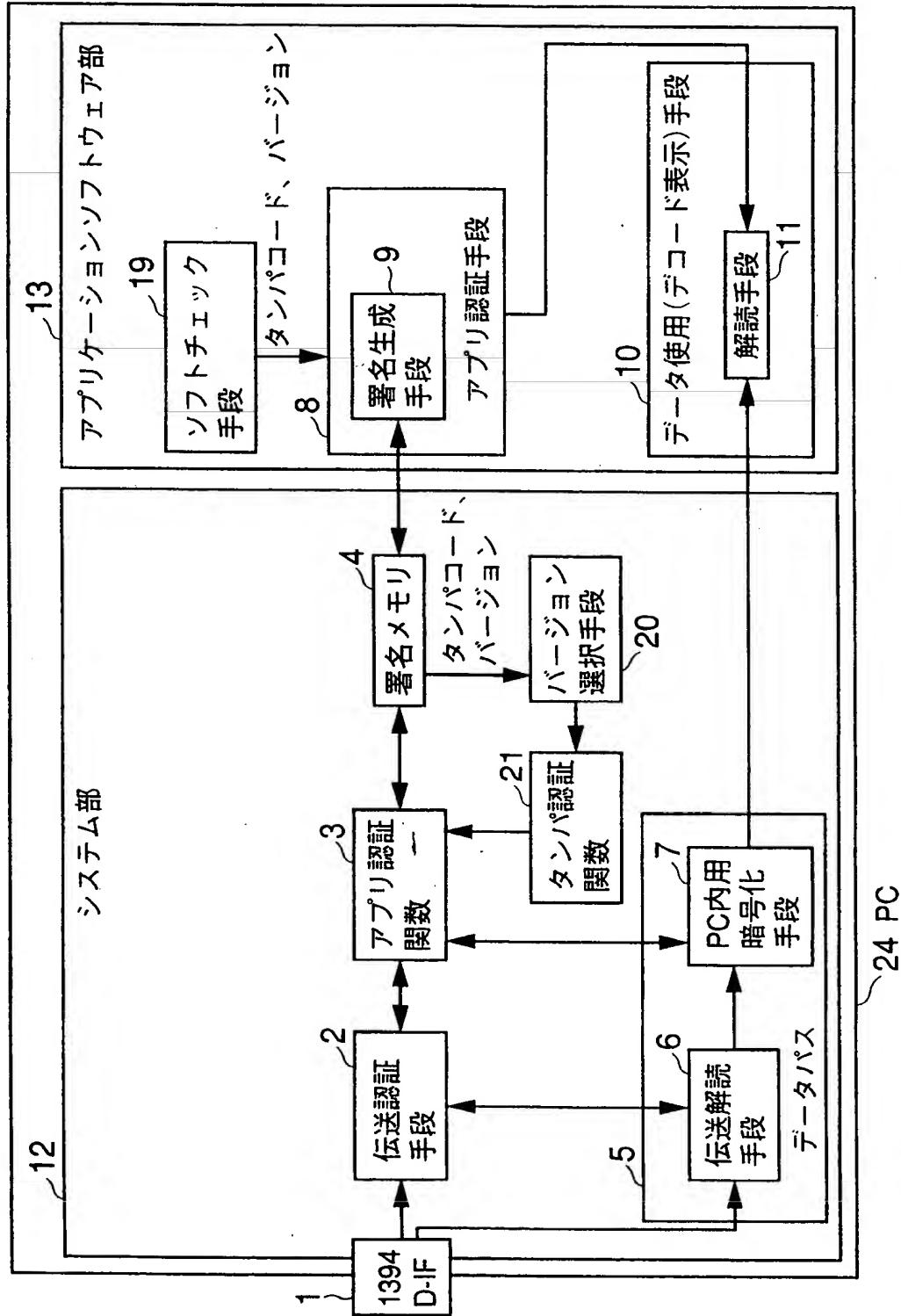
THIS PAGE BLANK (USPTO)

四三
第



THIS PAGE BLANK (USPTO)

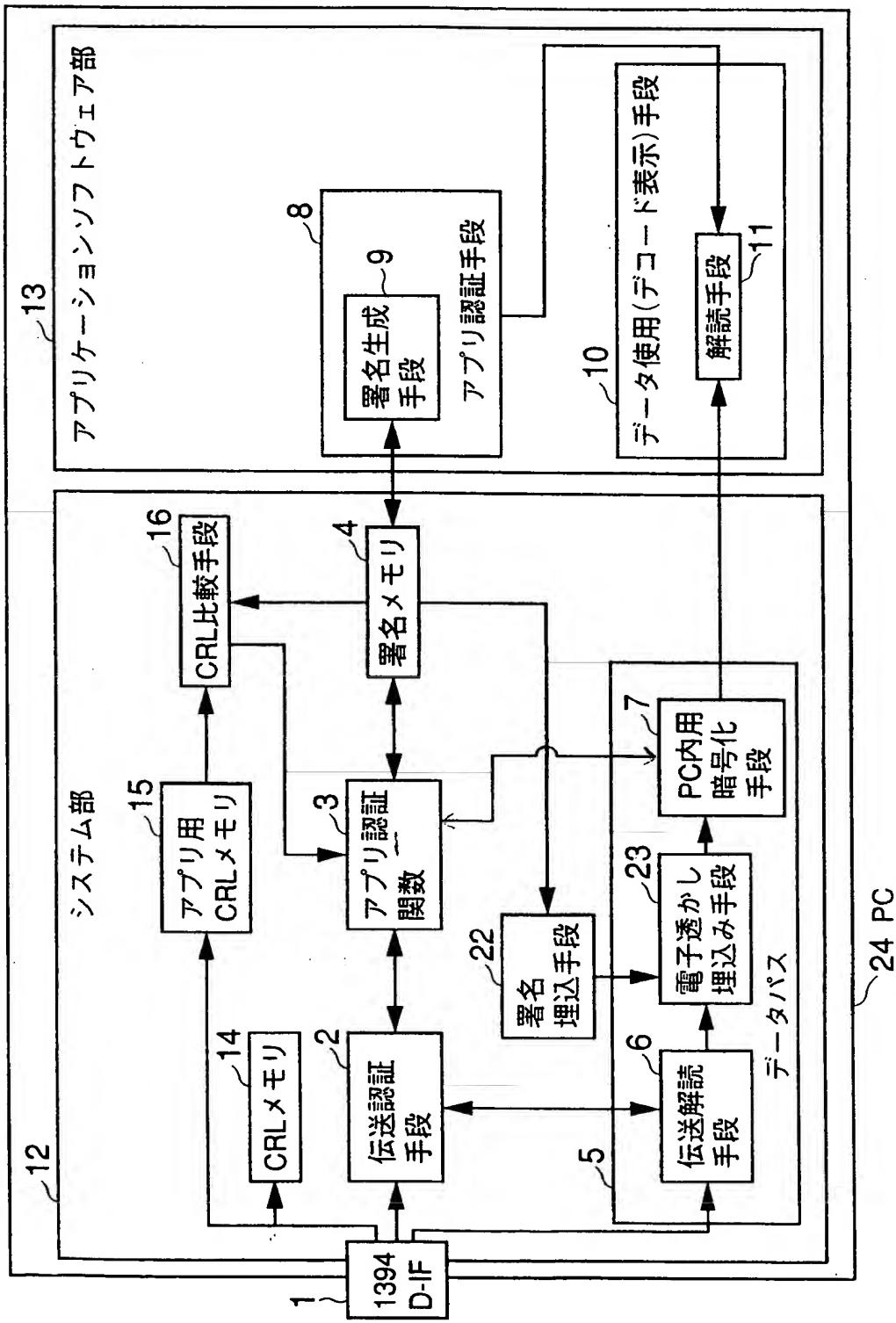
第4図



24 PC

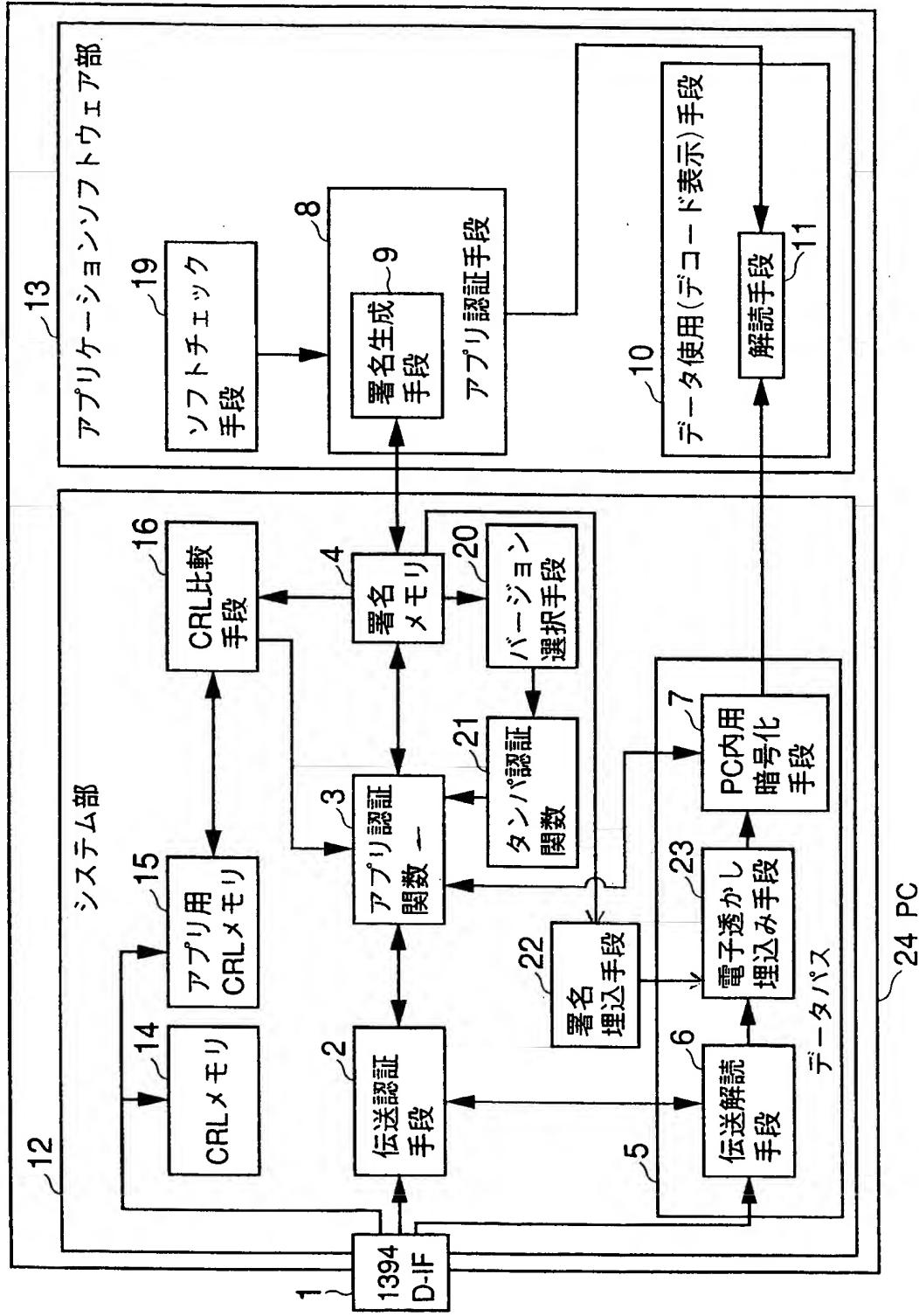
THIS PAGE BLANK (USPTO)

第5図



THIS PAGE BLANK (USPTO)

第6図



THIS PAGE BLANK (USPTO)

7 / 7

第7図

AVデータの著作権	アプリケーション ソフトウェアのライセンス	認証
複製禁止	A	成功
複製禁止	B	失敗
複製禁止	C	成功
一回のみ複製許可	A	成功
一回のみ複製許可	B	失敗
一回のみ複製許可	C	成功
これ以上の複製は不許可	A	成功
これ以上の複製は不許可	B	失敗
これ以上の複製は不許可	C	成功

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/00956

A. CLASSIFICATION OF SUBJECT MATTER

IntC17 G06F9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IntC17 G06F9/06-44, 12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI (INSPEC), JICST (JOIS)
DVD, IEEE1394, Copyright, Protection, Contents, Copyright Protection

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Nikkei Electronics, No.706, 05.January.1998 (Tokyo), David Aucsmith,	1-2,9
Y	"Gyaku Kaiseki ya Kaihen kara Soft wo mamoru Tanpa · Resistant · Software Gijutsu no Syousai",p.209-220	3-8
X	Nikkei Electronics, No.696, 18.August.1997(Tokyo), "DVD, PC ni noru Software Fukugou no Kagi wo nigiru Fusei Copy Boushi Gijyutsu no Medo",p.110-119	1-2,9
Y	The Institut of Image Information and Television Engineers, technical report, vol.21, No.31, 22.May.1997(Tokyo), Natsume MATSUZAKI, Hideshi ISHIHARA, Takahisa HUKUSHIMA, "DVD Copyright Protection System",p.15-19	1-8,9
Y	National TECHNICAL REPORT, vol.43, No.3, 18.June.1997 (Tokyo), Natsume MATSUZAKI, Makoto TATEBAYASHI, Hideshi ISHIHARA, Takahisa HUKUSHIMA, "DVD Copyright Protection System",p.118-122	1-9

Further documents are listed in the continuation of Box C.

See patent family annex.

• Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier document but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
31 March, 2000 (31.03.00)

Date of mailing of the international search report
18.04.00

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/00956

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	National TECHNICAL REPORT, vol.43, No.3, 18.June.1997, (Tokyo), Masakazu MATSUYAMA, Takatoshi MATSUI, Yukio MATSUURA, Eiki TAKAHASHI, "DVD-ROM Drive Tousai PC CF-200DV", p.31-35	1-9
Y	EP, 0875813, A2 (Sony Corp.), 01 November, 1998 (01.11.98), Full text; Figs. 1-24 & JP, 10-301492, A	1-9
A	WO, 96/41468, A1 (Macrovision Corp.), 22 June, 1996 (22.06.96), Full text; Figs. 1-13 & JP, 11-507160, A	1-9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/00956

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.: 10
because they relate to subject matter not required to be searched by this Authority, namely:
The constituent features described in claim 10 corresponds to a computer product by itself.
2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest The additional search fees were accompanied by the applicant's protest.
 No protest accompanied the payment of additional search fees.

THIS PAGE BLANK (USPTO)

国際調査報告

国際出願番号 PCT/JP00/00956

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int C17 G06F9/06

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))
Int C17 G06F9/06~44, 12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2000年
日本国登録実用新案公報 1994-2000年
日本国実用新案登録公報 1996-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI (INSPEC), JICST (JOIS)
DVD, IEEE1394, Copyright, Protection, Contents, 著作権保護

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	日経エレクトロニクス, 第706号, 05.1月. 1998(東京), David Aucsmitt h, "逆解析や改変からソフトを守る タンパ・レジスタント・ソフト ウェア技術の詳細", p. 209-220	1-2, 9
Y	日経エレクトロニクス, 第696号, 18.8月. 1997(東京), "DVD、パソ コンに載る ソフトウェア復号のカギを握る不正コピー防止技術の メド", p. 110-119	3-8
X	映像情報メディア学会技術報告, 第21巻, 第31号, 22.5月. 1997(東 京), 松崎なつめ, 石原秀志, 福島能久, "DVD著作権保護システム", p. 15-19	1-2, 9
Y		3-8
Y		1-8, 9

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示す
もの
「E」国際出願日前の出願または特許であるが、国際出願日
以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行
日若しくは他の特別な理由を確立するために引用する
文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって
出願と矛盾するものではなく、発明の原理又は理
論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明
の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以
上の文献との、当業者にとって自明である組合せに
よって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日
31.03.00

国際調査報告の発送日
18.04.00

国際調査機関の名称及びあて先
日本国特許庁 (ISA/JP)
郵便番号 100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)
田川 泰宏
電話番号 03-3581-1101 内線 3545
5B 4236

C (続き) 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	National TECHNICAL REPORT, 第43巻, 第3号, 18. 6月. 1997(東京), 松崎なつめ, 館林誠, 石原秀志, 福島能久, "DVD著作権保護システム", p. 118-122	1-9
Y	National TECHNICAL REPORT, 第43巻, 第3号, 18. 6月. 1997(東京), 松山雅一, 松井孝利, 松浦幸雄, 高橋英基, "DVD-ROMドライブ搭載パソコンCF-200DV", p. 31-35	1-9
Y	EP, 0875813, A2 (Sony Corp.), 04. 11月, 1998(01. 11. 98), 全文, 第1～第24図 &JP, 10-301492, A	1-9
A	WO, 96/41468, A1 (Macrovision Corp.), 22. 6月. 1996, (22. 06. 96), 全文, 第1～第13図 &JP, 11-507160, A	1-9

第I欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（PCT17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. 請求の範囲 10 は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
請求の範囲第10項に記載された構成は、コンピュータプログラム自体である。

2. 請求の範囲 _____ は、有意義な国際調査をできる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3. 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第II欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

1. 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2. 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3. 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4. 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

追加調査手数料の納付と共に出願人から異議申立てがあった。

追加調査手数料の納付と共に出願人から異議申立てがなかった。

THIS PAGE BLANK (USPTO)

特許協力条約

PCT

E P

U S

国際調査報告

(法8条、法施行規則第40、41条)
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 P22342-P0	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220) 及び下記5を参照すること。	
国際出願番号 PCT/JP00/00956	国際出願日 (日.月.年) 21.02.00	優先日 (日.月.年) 22.02.99
出願人(氏名又は名称) 松下電器産業株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 4 ページである。

この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
 この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
 この国際出願に含まれる書面による配列表
 この国際出願と共に提出されたフレキシブルディスクによる配列表
 出願後に、この国際調査機関に提出された書面による配列表
 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. 請求の範囲の一部の調査ができない(第I欄参照)。

3. 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は 出願人が提出したものを承認する。

次に示すように国際調査機関が作成した。

5. 要約は 出願人が提出したものを承認する。

第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1ヶ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、
第 1 図とする。 出願人が示したとおりである。

なし

出願人は図を示さなかった。

本図は発明の特徴を一層よく表している。

THIS PAGE BLANK (USPTO)